SECURITY INCIDENT REPORT AND RESPONSE PROCEDURES

As required by the Policy 552.01, suspected and actual breaches of security must be reported to the Los Angeles County Department of Mental Health (LACDMH) Help Desk or the Departmental Information Security Officer (DISO).

1. Organization of Emergency Response Teams

The DISO or his/her designee must represent the Department at the Countywide Computer Emergency Response Team (CCERT) as the primary Departmental Computer Emergency Response Team (DCERT) member.

LACDMH must organize a DCERT. The DISO will designate primary DCERT members and alternate members. Each DCERT member will actively participate in training and CERT activities at the Department and County level.

The DISO or his/her designee will update the CCERT with this contact information. The DISO must maintain current contact information for all personnel who are responsible for managing information technology (IT) resources to be utilized to remediate security threats.

LACDMH must provide the primary and secondary DCERT members with adequate portable communication devices (e.g., cell phone, pager)

DCERT must adopt and adhere to County policies, procedures, and guidelines pertaining to computer security threat response.

2. Security Incident Response and Report Procedure

A. Definition

According to Health Insurance Portability and Accountability Act of 1996, Security Rule, 164.304, a "security incident" means:

"the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system."

B. Pre-Incident

Incident handling is a generalized term that refers to the response by a person or LACDMH facility to an attack on a LACDMH information system and/or the information it contains. An organized and careful reaction to an incident can mean the difference between complete recovery and total disaster. The purpose of having incident handling procedures is to know what to do when an incident occurs. This means anticipating scenarios before they happen and making many decisions about them in advance.

To assist facility Workforce Members and others in knowing what to do when an incident occurs, LACDMH must prepare and maintain a Security Incident Response Matrix as a part of the process of implementing the LACDMH Security Compliance Program. This matrix recommends a response based on the type of computer security threat and the potential impact to LACDMH. In the matrix, a narrative of the required response must be placed in each cell corresponding to the intersection of the type of threat and the level of impact to the facility.

The Security Incident Response Matrix is a tool that the DCERT uses when confronted with a security incident and that shows the type of response that is required.

C. Post-Incident

DCERT response to computer security threats will consist of the following:

a. Identification
b. Isolation
c. Notification
d. Evaluation
e. Mitigation
f. Assessment
g. Reporting
h. Follow-Up

a. **Identification**

LACDMH Workforce Member must immediately report any and all suspected and actual breaches of information security (i.e., confidentiality, integrity, or availability) to his/her supervisor and the LACDMH Help Desk or DISO. Once a problem has been reported and the DCERT activated, the first priority for the DCERT is to determine the type, scope, and status of the incident, as DCERT's response is dependent upon the severity of the event. Each LACDMH facility must comply with all County policies for preservation of evidence and notification of appropriate authorities.

A LACDMH Incident Report form must be completed for each incident reported to DCERT.

b. **Isolation**

Affected systems must be immediately isolated from the rest of the network. During a wide-scale attack, isolation will frequently be done at the network level via routing and/or filtering components. LACDMH must comply with all County policies for preservation of evidence and notification of appropriate authorities.

The DISO or his/her designee and DCERT representatives have the authority and the responsibility to take necessary corrective action to remediate a computer security threat while preserving evidence related to the breach, as appropriate.

c. **Notification**

If the security incident is a Countywide security threat, then the DCERT must inform the DISO and the CCERT, as early as possible, of computer security threat events that could adversely impact Countywide computer systems and/or data. LACDMH must comply with the Board of Supervisors Policy 6.103, Countywide Computer Security Threat Responses and the Board of Supervisors Policy 6.101, Use of County Information Technology Resources for notification of appropriate authorities when violation of County IT resources is identified.

If the security incident is a LACDMH security threat then the DCERT must inform the DISO, as early as possible, of computer security threat events that could adversely impact LACDMH computer systems and/or data. The DCERT must also ensure notification of all other DMH facilities and/or persons of computer security threat events, e.g., LACDMH CIO, System Managers/Owners. The DCERT must also notify the LACDMH Privacy Officer if the security incident involves Protected Health Information.

Each facility must have in place a notification process to manage computer security threats within and outside their facility (including notification of, e.g., vendors, business associates, and State/Federal contacts).

d. **Evaluation**

Once a LACDMH computer security threat has been identified and the DCERT activated, evaluation must begin to determine the steps necessary to mitigate the threat. The evaluator must recommend to the DCERT a course of action and the DCERT will either act on the recommendation or modify it as necessary.

LACDMH must comply with all County policies for preservation of evidence and notification of appropriate authorities.

e. **Mitigation**

After the DCERT has endorsed recommended course of action, remediation information will be communicated to all facilities. DCERT members must then rapidly implement the recommended course of action.

f. **Assessment**

During a computer security threat, each DCERT representative must document the number of affected systems within their organization in the LACDMH Incident Report.

The LACDMH facility impact of any such incident should also be assessed and documented by the DCERT representative in terms of downtime, impacted services, and quantifiable resources expended to mitigate the threat.

g. **Reporting**

The DCERT representative must forward to the DISO information generated by assessment within five (5) working days following a LACDMH computer security threat. Within ten (10) working days of any such incident, the DCERT will develop an event chronology that will be presented to the DISO.

h. **Follow-Up**

After the threat has been contained and the majority of LACDMH systems have been restored to normal operation, a postmortem analysis will be performed. In order to remain effective, the DCERT will discuss amongst its members the actions taken, derive "lessons learned" and modify existing Guidelines and Procedures, if necessary.